PAT-NO: JP402199939A
DOCUMENT-IDENTIFIER: JP 02199939 A
TITLE: SYSTEM FOR VERIFYING OPPOSITE PARTY
PUBN-DATE: August 8, 1990
INVENTOR-INFORMATION:
NAME
SONEDAKA, NORIYOSHI
INT-CL (IPC): H04L009/00, G09C001/00 , H04L009/10 , H04L009/12

ABSTRACT:

PURPOSE: To secure the confidentiality even when an ID number of one party is intercepted by a 3rd party and to detect the presence of a forged data by the 3rd party immediately by using both receiver and sender ID numbers.

CONSTITUTION: A basic decoding section D1 decodes a sender ID number by using a secret key S4 in common to the sender and the receiver. The secret hey S4 is obtained by a selection section D1-2 selecting either a secret key S3 outputted from a secret key register section D3 or a receiver ID number S6 outputted from a receiver ID number register section D4. Then a decoded signal S5 is decoded by using the receiver ID number S4 and the decoded signal is outputted to a transmission line T1. A basic cryptographic section E1 of the receiver side ciphers the decoded signal S7 by using the receiver ID number S4. A decoded signal S8 generated from the basic cryptographic section E1 is inputted to a sender ID number verification section E2, in which a sender ID number outputted from a sender ID number register section D2 and the decoded signal S8 are compared.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2−199939

⑤1Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)8月8日
H 04 L 9/00			
G 09 C 1/00		7368−5B	
H 04 L 9/10			
9/12			
		6945−5K　H 04 L 9/00　Z	

審査請求　未請求　請求項の数 1　(全6頁)

⑭発明の名称　相手認証方式

⑳特　願　平1−18908
㉒出　願　平1(1989)1月28日

⑫発明者　曽根高　則義　東京都港区芝5丁目33番1号　日本電気株式会社内
⑪出願人　日本電気株式会社　東京都港区芝5丁目7番1号
⑭代理人　弁理士　芦田　坦　外2名

明　細　書

1．発明の名称

相手認証方式

2．特許請求の範囲

1)　任意の通信路において、送信者が通信文をディジタル署名して受信者が確認する相手認証方式であって、送信者側は、nビット(nは自然数)からなる送信者ID番号IDiを受信者側と共通に取り決めたnビットからなる秘密鍵MKで復号化する所定のアルゴリズムによりnビットからなる復号化信号Ciを生成する手段と、前記復号化信号Ciを、nビットからなる受信者ID番号IDjで復号化する所定のアルゴリズムによりnビットからなる復号化信号Cijを生成する手段と、該復号化信号Cijを伝送路に送出する手段とを有し、受信者側は、前記伝送路から受信した復号化信号Cij'をnビットからなる受信者ID番号IDjにて暗号化する所定のアルゴリズムによりnビットからなる暗号化信号Ci'を生成する手段と、前記暗号化信号Ci'を、送信者側と共通に取り決めたnビットからなる秘密鍵MKで暗号化する所定のアルゴリズムによりnビットからなる送信者ID番号IDi'を生成する手段と、送信されてくる送信者ID番号IDi'と認識している送信者ID番号とが一致するかどうかを判別する手段とを有することを特徴とする相手認証方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、任意の通信路において送信者が通信文をディジタル署名して受信者が確認する相手認証方式に関する。

〔従来の技術〕

この種の相手認証方式については、例えば社団法人電子通信学会から昭和61年に発行された刊行物"現代暗号化理論"(217頁から239頁)にいくつかの例が示されている。

第1の例は、送信者側のID番号を送／受信者

共通の秘密鍵で復号化して送出し、受信側では秘密鍵で復号化された信号より送信者側のＩＤ番号を得る方式である。

第２の例では送信者側が送信者側のＩＤ番号を受信側に平文で送出し、その後、送信者のＩＤ番号を送／受信者共通の秘密鍵でハッシュ関数ｈを施し、別の秘密鍵で復号化して受信側に送出する。この第２の例では、受信者側は、最初に送出されたＩＤ番号を共通秘密鍵でハッシュ関数ｈを施して得られる値と、後に送られてくるＩＤ番号をハッシュ関数ｈで圧縮して復号化した信号を別の秘密鍵で暗号化することにより得られる値とが一致するかどうか比較して相手を認証する。

第２図を参照して上記第１の方式について説明する。

まず、送信者側では、送信者ＩＤ番号レジスタ部Ｄ２より出力される送信者ＩＤ番号（ＩＤ１）Ｓ１と秘密鍵レジスタ部Ｄ３より出力される秘密鍵（ＭＫ）Ｓ４を基本復号化部Ｄ１によって復号化した後、復号化信号Ｓ５を伝送路Ｔ１に出力する。

伝送路Ｔ１を経由して受信者側には復号化信号Ｓ６が供給される。送信者側にあるものと同じ秘密鍵レジスタ部Ｄ３より出力される秘密鍵（ＭＫ）Ｓ４を用いて復号化信号Ｓ６を基本暗号化部Ｅ１によって暗号化した後、送信者ＩＤ番号認証部Ｅ２に復元信号（ＩＤ１′）Ｓ８として出力する。送信者ＩＤ番号認証部Ｅ２は、期待する相手の送信者ＩＤ番号レジスタ部Ｄ２からの送信者ＩＤ番号Ｓ１と復元信号Ｓ８とを比較し、一致していれば認証結果信号Ｓ９を出力する。

この認証方式は、送信側において、

$$D(MK, ID1) = C1 \quad \cdots (2\text{-}1)$$

受信側において、

$$E(MK, C1) = ID1' \quad \cdots (2\text{-}2)$$

期待する認証は、

$$ID1 = ID1' \quad (\text{但し、} D = E^{-1}) \quad \cdots (2\text{-}3)$$

ならば、相手を認証したとする方式である。

もしも、第３者において改ざん等が実施されていれば、

$$ID1 \neq ID1' \quad \cdots (2\text{-}4)$$

となる。

第３図は前述した第２の方式の構成例を示す。この方式は、送信者側で手順１として、送信者ＩＤ番号レジスタ部Ｄ２より出力される送信者ＩＤ番号（ＩＤ１）Ｓ１を伝送路Ｔ１に送出する。次に、手順２として、送信者ＩＤ番号Ｓ１を秘密鍵レジスタ部Ｄ３から出力される秘密鍵（ＭＫ）Ｓ４を使用してデータ圧縮部Ｈ１においてハッシュ関数ｈを施し、圧縮信号Ｓ１１として基本復号化部Ｄ１に出力する。基本復号化部Ｄ１では入力した圧縮信号Ｓ１１を他の秘密鍵レジスタ部Ｄ５より出力された秘密鍵（ＭＫ２）Ｓ１０で復号化し、復号化信号（Ｃ１）Ｓ１２として伝送路Ｔ１に出力する。

伝送路Ｔ１を経由して受信者側には送信者ＩＤ番号Ｓ１による送信者ＩＤ番号Ｓ１３と復号化信号Ｓ１２による復号化信号Ｓ１４が供給される。

受信者側では、手順１として、受信した送信者ＩＤ番号（ＩＤ１′）Ｓ１３を送信者側にあるものと同じ秘密鍵レジスタ部Ｄ３より出力される秘密鍵（ＭＫ）Ｓ４で送信者にあるものと同じデータ圧縮部Ｈ１においてハッシュ関数ｈを施した後、圧縮信号（Ｃｈ１′）Ｓ１１として送信者ＩＤ番号認証部Ｅ２に出力する。

次に、手順２として、受信した復号化信号（Ｃ１′）Ｓ１４に対して送信者側のものと同じ他の秘密鍵レジスタ部Ｄ５により出力される秘密鍵（ＭＫ２）Ｓ１０を用いて基本暗号化部Ｅ１において暗号化を施した後、復元信号（Ｃｈ１′）Ｓ１５として送信者ＩＤ番号認証部Ｅ２に出力する。送信者ＩＤ番号認証部Ｅ２では、圧縮信号Ｓ１１と復元信号Ｓ１５とを比較し、一致していれば相手認証として認証結果信号Ｓ９を出力する。

この認証方式は次式で証明できる。

送信側において、

手順１：$H(MK, ID1) = Ch1 \quad \cdots (3\text{-}1)$

手順２：$D(MK2, Ch1) = C1 \quad \cdots (3\text{-}2)$

受信側において、

手順１：Ｈ（ＭＫ，ＩＤｉ′）＝Ｃｈｉ′
…(3-3)

手順２：Ｅ（ＭＫ２，Ｃｉ′）＝Ｃｈｉ′
…(3-4)

ここで、送信者ＩＤ番号認証部Ｅ２は、

Ｃｈｉ′＝Ｃｈｉ′ …(3-5)

ならば、相手認証したとする。

もしも、第３者において改ざん等が実施されていれば、

Ｃｈｉ′≠Ｃｈｉ′ …(3-6)

となり、改ざん等の有無か期待する相手ではないかの判定ができる。

［発明が解決しようとする課題］

上記第１の方式においては、２者間以上の相手との交信に共通の秘密鍵を使用する場合、(2-3)式が成立しても、送信側は期待した受信側と交信ができるとは限らない欠点がある。

また、伝送路Ｔ１において、送信信号に伝送路品質劣化の影響が存在する場合、(2-3)式が成立しても相手を認証したとはならない欠点がある。

一方、第２の方式においては、第１の方式の欠点の一部は解決されるものの、送信者ＩＤ番号が平文で伝送路に送出されるため、第３者による“なりすまし”が存在する可能性がある。また、第１の方式と同様２者間以上の相手の交信に於いて、(3-5)式が成立しても期待する受信側との交信が期待できたとはならない過大なる欠点が存在していた。

［課題を解決するための手段］

本発明は、任意の通信路において、送信者が通信文をディジタル署名して受信者が確認する相手認証方式であって、送信者側は、ｎビット（ｎは自然数）からなる送信者ＩＤ番号ＩＤｉを受信者側と共通に取り決めたｎビットからなる秘密鍵ＭＫで復号化する所定のアルゴリズムによりｎビットからなる復号化信号Ｃｉを生成する手段と、前記復号化信号Ｃｉを、ｎビットからなる受信者ＩＤ番号ＩＤｊで復号化する所定のアルゴリズムによりｎビットからなる復号化信号Ｃｉｊを生成する手段と、該復号化信号Ｃｉｊを伝送路に送出する手段とを有し、受信者側は、前記伝送路から受信した復号化信号Ｃｉｊ′をｎビットからなる受信者ＩＤ番号ＩＤｊにて暗号化する所定のアルゴリズムによりｎビットからなる暗号化信号Ｃｉ′を生成する手段と、前記暗号化信号Ｃｉ′を、送信者側と共通に取り決めたｎビットからなる秘密鍵ＭＫで暗号化する所定のアルゴリズムによりｎビットからなる送信者ＩＤ番号ＩＤｉ′を生成する手段と、送信されてくる送信者ＩＤ番号ＩＤｉ′と認識している送信者ＩＤ番号とが一致するかどうかを判別する手段とを有することを特徴とする。

本発明によれば、送信者側における復号化のアルゴリズムは、

Ｄ（ＭＫ，ＩＤｉ）＝Ｃｉ …(1)

Ｄ（ＩＤｊ，Ｃｉ）＝Ｃｉｊ …(2)

で表わされ、受信者側における暗号化のアルゴリズムは、

Ｅ（ＩＤｊ，Ｃｉｊ′）＝Ｃｉ′ …(3)

Ｅ（ＭＫ，Ｃｉ′）＝ＩＤｉ′ …(4)

で表わされる。

［実施例］

第１図を参照して本発明の一実施例を説明する。

送信者側は、手順１において次のように動作する。

基本復号化部Ｄ１によって、送信者ＩＤ番号Ｓ２を送／受信共通の秘密鍵Ｓ４で復号化する。ここで、基本復号化部Ｄ１は、例えばＤＥＳ(DATA ENCRYPTION STANDERD)のような慣用暗号化アルゴリズムを有したものである。また、送信者ＩＤ番号Ｓ２は、送信者ＩＤ番号レジスタ部Ｄ２から出力された送信者ＩＤ番号Ｓ１と基本復号化部Ｄ１からの出力を戻すことにより得られる復号化信号Ｓ５との一方を選択する選択部Ｄ１－１により得られる。手順１においては送信者ＩＤ番号Ｓ１を選択したものである。更に、秘密鍵Ｓ４は、秘密鍵レジスタ部Ｄ３から出力された秘密鍵Ｓ３と受信者ＩＤ番号レジスタ部Ｄ４から出力された受信者ＩＤ番号Ｓ６の一方を選択する選択部Ｄ１－２により得られる。手順１においては秘密鍵Ｓ３を選択したものである。

基本復号化部Ｄ１より復号化された復号化信号Ｓ５は、選択部Ｄ１－３によって選択部Ｄ１－１に戻る経路を選択される。

手順２においては次のように動作する。

基本復号化部Ｄ１によって復号化信号Ｓ５を受信者ＩＤ番号Ｓ４で復号化する。第１の選択部Ｄ１－１は復号化信号Ｓ５を選択してＳ２とし、選択部Ｄ１－２は受信者ＩＤ番号Ｓ６を選択してＳ４とする。また、選択部Ｄ１－３は手順２で生成された復号化信号Ｓ５を選択し、伝送路Ｔ１に出力する。伝送路Ｔ１を通過した復号化信号は復号化信号Ｓ７として受信者側に入力する。

受信者側は手順１において次のように動作する。

基本暗号化部Ｅ１によって復号化信号Ｓ７を受信者ＩＤ番号Ｓ４で暗号化する。ここで、受信者ＩＤ番号Ｓ４は、送信者側のものと同じ受信者ＩＤ番号レジスク部Ｄ４から出力された受信者ＩＤ番号Ｓ６と送信者側のものと同じ秘密鍵レジスタ部Ｄ３から出力される秘密鍵Ｓ３との一方を選択する選択部Ｅ１－２に入力され、手順１においては受信者ＩＤ番号Ｓ６を選択したものである。また、復号化信号Ｓ７は、送信者側のものと同じ基本暗号化部Ｅ１からの出力を戻すことにより得られる復元信号Ｓ８と伝送路Ｔ１を通して受信した復号化信号Ｓ７との一方を選択する選択部Ｅ１－１に入力され、手順１においては、復号化信号Ｓ７を選択する。基本暗号化部Ｅ１によって復元された復元信号Ｓ８は、選択部Ｅ１－３で選択部Ｅ１－１に戻る経路を選択される。

手順２においては次のように動作する。基本暗号化部Ｅ１によって、復号化信号Ｓ７を秘密鍵Ｓ４で暗号化する。選択部Ｅ１－１は手順１で生成された復元信号Ｓ８を、選択部Ｅ１－２においては秘密鍵Ｓ３を、選択部Ｅ１－３では送信者ＩＤ番号認証部Ｅ２に送出する経路を選択してある。

基本暗号化部Ｅ１より生成された復元信号Ｓ８は、送信者ＩＤ番号認証部Ｅ２に入力される。送信者ＩＤ番号認証部Ｅ２において、送信者ＩＤ番号レジスタ部Ｄ２より出力された送信者ＩＤ番号Ｓ１と復元信号Ｓ８を比較し、一致しているかどうかの結果を認証結果信号Ｓ９として出力する。

１例として、送信する信号の平文を送信者ＩＤ番号としたが、特に送／受信者間で任意に取り決めたディジタル署名文でもよい。

［発明の効果］

以上説明したように、本発明の相手認証方式は、受信者と送信者のＩＤの両方を使用する事から、一方のＩＤ番号が第３者に分かっても秘密は保持でき、第３者の改ざん等の有無も即座に検出できる。

４．図面の簡単な説明

第１図は、本発明の一実施例に係る相手認証方式の構成例である。

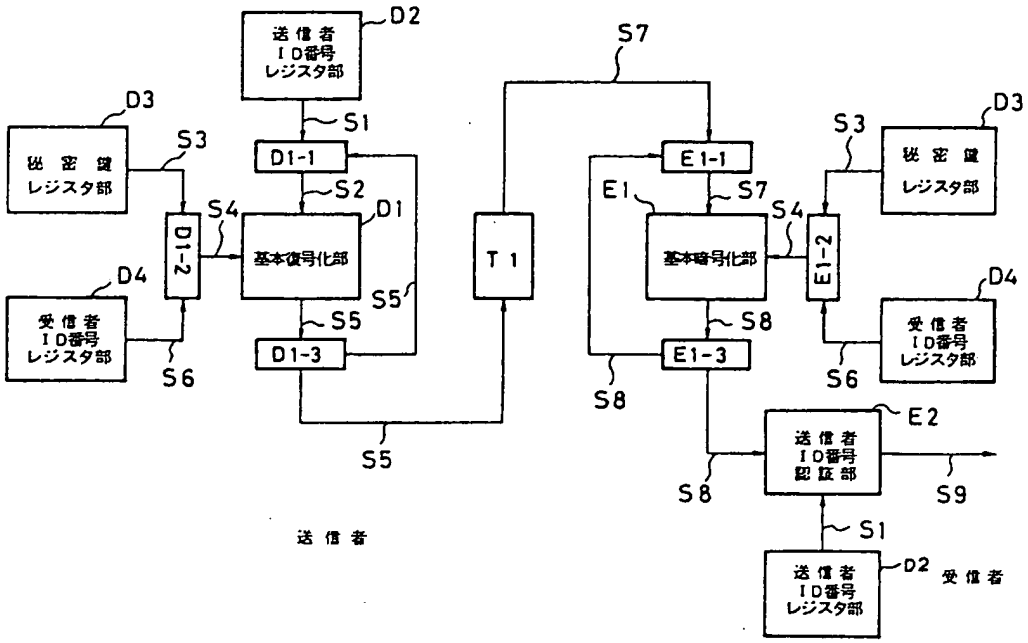
第２図は、従来の相手認証方式の一例を示す構成例である。

第３図は、従来の相手認証方式の他の構成例である。

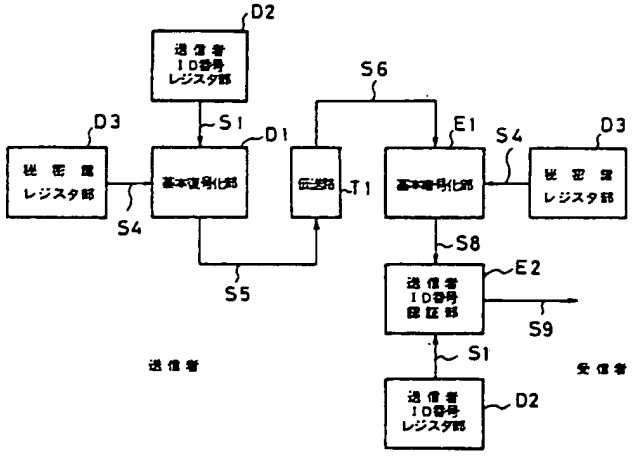
Ｄ１…基本復号化部、Ｄ２…送信者ＩＤ番号レジスタ部、Ｄ３…秘密鍵レジスタ部、Ｄ４…受信者ＩＤ番号レジスタ部、Ｄ５…秘密鍵レジスタ部、Ｅ１…基本暗号化部、Ｅ２…送信者ＩＤ番号認証部。

代理人 (7783) 弁理士 池田憲保

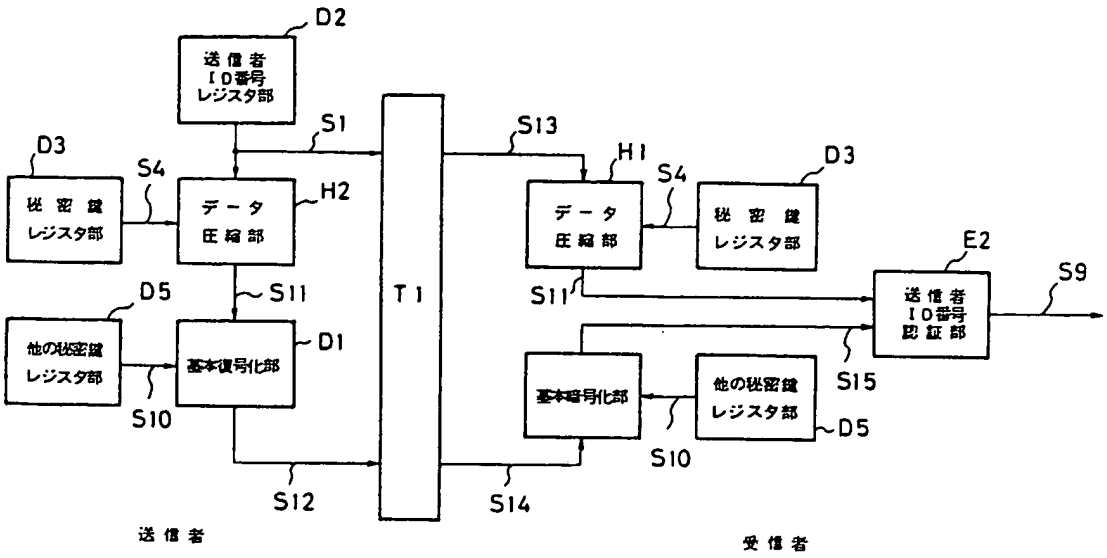
第 1 図


送信者 ID番号 レジスタ部
D2
S1
D1-1
S2
D1
基本復号化部
S5
D1-3
S5
D1-2
S4
秘密鍵 レジスタ部
D3
S3
受信者 ID番号 レジスタ部
D4
S6
T 1
S7
E1-1
E1
S7
基本暗号化部
S8
E1-3
S8
E1-2
S4
S3
秘密鍵 レジスタ部
D3
D4
受信者 ID番号 レジスタ部
S6
E2
送信者 ID番号 認証部
S8
S9
S1
送信者 ID番号 レジスタ部
D2
送信者
受信者

第 2 図


D2
S6
D3
S1
D1
E1
S4
D3
S4
T1
S5
S8
E2
S9
S1
D2
送信者
受信者

第 3 図


D2
送信者
ID番号
レジスタ部
S1
S13
D3
S4
秘密鍵
レジスタ部
データ
圧縮部
H2
H1
S4
D3
データ
圧縮部
秘密鍵
レジスタ部
E2
S9
D5
S11
T1
S11
送信者
ID番号
認証部
他の秘密鍵
レジスタ部
基本復号化部
D1
S15
基本暗号化部
他の秘密鍵
レジスタ部
S10
S10
D5
S12
S14
送信者
受信者